ATTORNEY DOCKET NO.
15927RRUS02U (NORTH 2874001)

PATENT APPLICATION
SERIAL NO. 10/780,007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of: Chowdhury et al.	§	Confirmation No. 9570
	§	
Serial Number: 10/780,007	§	
	§	Group Art Unit: 2169
Filed: February 17, 2004	§	
	§	
For: DISCOVERY OF APPLICATION SERVER IN AN IP NETWORK	§	Examiner: Kim, Paul
	§	

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 37 C.F.R. § 1.8, I hereby certify that this correspondence is being electronically transmitted to the United States Patent and Trademark Office at www.uspto.gov

on: June 15, 2010

/Bradley D. Ellis/
Bradley D. Ellis

Via EFS-Web
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPELLANT'S APPEAL BRIEF

Appellant respectfully submits this brief in support of the patentability of the claims of the above-referenced application.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is Nortel Networks Limited, the assignee of record.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

The application contains Claims 1-6 and 15-20. Claims 1-3, 15, and 20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,970,924 to Chu et al. ("Chu") in view of U.S. Patent No. 7,225,272 to Kelley et al. ("Kelley"), and in further view of U.S. Patent No. 7,349,894 to Barth et al. ("Barth"). Claims 4-6 and 16-19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Chu, in view of Kelley and Barth, and in further view of Official Notice. Appellant appeals the Examiner's rejections of Claims 1-6 and 15-20.

IV. STATUS OF AMENDMENTS

A claim amendment was filed on June 10, 2010, to present the rejected claims in better form for consideration on appeal. This amendment has not been entered. The amendment does not change the scope of any claim, and instead merely makes clear that the serving network domain name in Claims 1 and 15 is extracted from the reverse domain name query response. This limitation is already apparent in Claims 1 and 15 in view of the specification and the limitation that the reverse domain name query response comprises the serving network domain name.

V. SUMMARY OF CLAIMED SUBJECT MATTER

A wireless mobile device, such as a mobile telephone, may be connected to a serving Internet Protocol network ("IP network"). Specification Fig. 1 refs. 103 and 111 and page 1, lines 14-18. The mobile device may use Internet Protocol to communicate with an application server on the IP network. Specification page 1, lines 17-27. The application server may provide a service to the wireless mobile device, such as prepaid voice, instant messaging, or broadcasting of information. Specification page 1, lines 22-24.

To communicate with the application server and receive the service, the wireless mobile device requires the Internet Protocol address ("IP address") of the application server. Specification page 2, lines 1-11. Each application server is specific to a particular IP network. Specification page 2, lines 4-5. When the mobile device connects to a new serving IP network and desires a particular service, the mobile device must discover the Internet Protocol address of an application server on the new IP network which can provide the service. Specification page 2, lines 4-11.

A device domain name is a textual name associated with an IP address. Specification page 7, lines 19-21. An example of a device domain name is "agw.xyz.com", and an example of an IP address is "123.567.888.143". Specification page 7, lines 18-21. A device domain name may be converted into a corresponding IP address through a domain name query such as a DNS query. Specification page 8, lines 6-11. An IP address may be converted into a corresponding device domain name through a reverse domain name query such as a reverse DNS query. Specification page 7, lines 23-24.

The present invention permits a mobile device to find the IP address of an application server providing a desired service. Specification page 4, line 30 to page 5, line 5. The mobile device may do so by utilizing two properties of IP networks. First, one part of an application server's domain

name, called the application server name, is standardized across IP networks, typically based on the service provided by the application server. Specification page 5, lines 20-25. Second, the other part of an application server's domain name, called the serving network domain name, is also part of the device domain names of other devices on the network. Specification page 5, lines 21-28 and page 6, lines 21-23.

Because the first part is typically standardized based on the service provided, the mobile device may select the first part as a function of the desired service. Specification page 7, line 30 to page 8, line 2. To obtain the second part, the serving network domain name, the mobile device may begin with a known IP address of a device on the serving IP network. Specification page 6, lines 5-6. This IP address may be the mobile device's own IP address or the IP address of an access gateway on the serving IP network. Specification page 6, lines 5-6 and 14-16. By performing a reverse domain name query on the known IP address, the mobile device may receive a device domain name which includes the serving network domain name. Specification page 6, lines 21-23.

By finding the two parts and appending the serving network domain name to the application server name, the mobile device may form the device domain name of the desired application server. Specification page 6, lines 23-25. The mobile device may then perform a domain name query to convert the device domain name into the IP address of the application server. Specification page 6, lines 26-31.

Independent Claim 1 recites a method of determining the IP address of the application server in accordance with the above. Independent Claim 15 recites a system comprising a wireless mobile device configured to determine the IP address of the application server in accordance with the above.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Whether Claims 1-3, 15, and 20 are unpatentable under 35 U.S.C. § 103(a) as being unpatentable over Chu in view of Kelley in further view of Barth.

B. Whether Claims 4-6 and 16-19 are unpatentable under 35 U.S.C. § 103(a) as being unpatentable over Chu, in view of Kelley and Barth, and in further view of Official Notice.

VII. ARGUMENT

A. Chu

The Office Action cites Chu as disclosing a reverse domain name query. Office Action page 7. Chu "relates to network monitoring and more specifically to network monitoring of end user experience." Chu col. 1, lines 7-9. As part of network monitoring, Chu teaches testing routers between two points. Chu col. 15, lines 20-28. Using the Internet Protocol Time-To-Live field and Record Route option, Chu builds a list of IP addresses of routers on paths between the two points. Chu col. 15, lines 29-65.

The Office Action cites a portion of Chu disclosing a technique for determining which of the routers are boundary routers. Chu col. 16, lines 7-32. A boundary router is a router which has links to routers with different network domain names[1]. Chu col. 16, lines 13-17. Chu teaches performing a reverse DNS query on the IP address of each link of a router. Chu col. 16, lines 10-13. If the links have different domain names, the router is a boundary router. Chu col. 16, lines 10-17. By determining which routers are boundary routers, domains can be associated with amounts of delay in the network. Chu col. 16, lines 26-32.

B. Barth

The Office Action cites Barth as teaching a domain name query. Office Action page 7. Barth teaches server load balancing. Barth col. 11, lines 19-26. Requests by clients are balanced

---

[1] For consistency, the application's terminology is used herein. The application uses the term "network domain name" to refer to what Chu calls a "domain name". For example, the specification at page 5, lines 25-27 refers to "abc.com" as a network domain name, analogous to the domain names "inverse.net" and "alter.net" at Chu col. 16, lines 14-17.

among multiple servers. Barth col. 11, lines 19-62. To contact a server, a client forms a server domain name from three string fragments. Barth col. 11, lines 27-37. One of the string fragments is a random integer between 0 and 99, causing the client to have an equal chance of forming any of 100 different server domain names.

In an example given in Barth, the first string fragment is "start", the second string fragment is the random integer between 0 and 99, and the third string fragment is ".somename.com". Barth col. 11, lines 27-37. The clients may therefore generate the server domain names "start00.somename.com", "start01.somename.com", "start75.somename.com", "start90.somename.com", and so on. Barth col. 11, lines 53-63.

After generating a server domain name, the client performs a DNS query on the server domain name and receives the IP address of the associated server. Barth col. 12, lines 7-13. Each of the multiple servers may have an IP address associated with one or more of the 100 server domain names. Barth col. 11, lines 46-63. Each server domain name a server's IP address is associated with causes approximately 1% of client traffic to be directed to the server. *See* Barth col. 12, lines 1-6.

C. Kelley

The Office Action also cites Kelley as teaching a domain name query. Office Action page 7. Kelley teaches a type of domain name query which is an alternative to DNS queries. Kelley col. 2, lines 56-67 and col. 3, lines 24-58. Kelley teaches the Kelley domain name queries are an improvement upon DNS queries because, unlike DNS queries, Kelley domain name queries do not require a database for mapping domain names to IP addresses. Kelley col. 2, lines 56-67 and col. 3, lines 24-58.

The processing of Kelley domain name queries differ from DNS queries in several respects. Kelley col. 3, lines 24-58. However, both forms of domain name queries receive a domain name as input and provide a numerical address as output. Kelley col. 3, lines 30-38 and 43-46.

D. 35 U.S.C. § 103(a) Rejection of Claim 1

1. The Cited DNS Query Would Have no Purpose

Independent Claim 1 recites "performing… a domain name query using the domain-specific application server name". The domain-specific application server name is generated by "appending… the extracted serving network domain name to the application server name". The extracted serving network domain name is extracted from the response to a reverse domain name query. In other words, *a domain name query is performed using the response to a reverse domain name query.*

Chu teaches only reverse domain name queries. Barth and Kelley teach only domain name queries. Therefore, the Office Action relies on the combination of Chu with Barth and Kelley to reject Claim 1, which recites both types of domain name queries. Office Action page 7. However, a combination of Chu and Barth or a combination of Chu and Kelley would not include a domain name query using the result of a reverse domain name query, because the domain name query would have no purpose.

Chu teaches monitoring the path between two points on a network. Chu builds a list of the IP addresses of the routers between the two points. To determine if a router is a boundary router, Chu teaches performing a reverse domain name query on the IP address of each router the router has links to. If the router has linked routers with different network domain names, the router is a boundary router.

At the time the reverse domain name queries are performed, therefore, Chu *already has the IP address of every router*. These are the same IP addresses the reverse domain name queries are performed on. According to the Office Action at page 7:

> The additional feature of using a domain name (returned from a reverse DNS query) in a domain name query would allow for the identification of an IP address associated with a specific application server name.

This statement overlooks the context of the reverse domain name queries performed in Chu. There is no reason to use a domain name query "for the identification of an IP address associated with a specific application server name." That same application server name was obtained from the very IP address the domain name query would identify. The cited references do not provide any reason why an already-identified IP address must be identified a second time.

2. The Cited Dynamic Generation of an Application Server Name Would Destroy the Principle of Operation of Chu

Claim 1 recites "appending, by the wireless mobile device, the extracted serving network domain name to the application server name, thereby generating a domain-specific application server name". Chu does not teach the generation of an application server name. Office Action page 3. The Office Action cites Barth as teaching the generation of an application server name. Office Action pages 3-4. However, dynamically generating an application server name as taught in Barth would destroy the principle of operation of Chu.

Barth teaches load balancing of client requests. A client directs its requests to one of 100 possible server domain names, which are associated with the IP addresses of multiple servers. Inherently, the different servers have different IP addresses. "[T]here is no requirement that the corresponding IP addresses have any commonality or relationship. This allows, for example, **the server identified by the host name 'start00.somename.com' to be at an entirely different**

physical location from the one named 'start01.somename.com.'" Barth col. 11, lines 46-56. (Emphasis added). Therefore, the IP addresses produced by the dynamic generation of an application server name may be at entirely unrelated locations.

The purpose of the reverse DNS queries in Chu is to determine responsibility for delay in a particular network path. Chu col. 16, lines 25-32. The purpose of using 100 different server domain names in Barth is to balance client requests. To randomly change a router domain name in Chu to one of 100 different domain names, associated with multiple different, unrelated IP addresses, defeats the purpose of network monitoring. As stated in Barth, the different IP addresses may be entirely unrelated. When monitoring the performance of a specific router, as taught in Chu, there is no reason to replace that router's IP address with the IP address of a randomly selected router as taught in Barth. The cited combination could not monitor any network path, because the random changing of IP addresses would randomly change the path being monitored, potentially to a router in an entirely different physical location having little relation to the original path.

3. Conclusion

Claim 1 requires a domain name query performed using the result of a reverse domain name query. The proposed combination of Chu, Barth, and Kelley at page 7 of the Office Action would perform a reverse DNS query on an IP address to obtain a domain name, and then perform a DNS query on the domain name to obtain that same IP address. The proposed combination would be redundant and have no purpose in Chu.

Claim 1 additionally requires the generation of a domain-specific application server name. In Chu, the relevant domain names are the domain names of routers on a path between two points. Barth teaches generating an application server name including a random integer between 0 and 99, causing the generation of one of 100 possible application server names. The application server

names may be associated with IP addresses of servers in entirely different locations. Accordingly, to generate an application server name as taught in Barth, using a router domain name as taught in Kelley, can produce the domain name of a router which is not part of the path being monitored. This potential substitution of a relevant router for an irrelevant router has no purpose in Chu.

In view of the foregoing, it is apparent that the combination of Chu, Barth, and Kelley does not teach the unique combination recited in Claim 1. Accordingly, Appellant respectfully requests that the rejection of Claim 1 under 35 U.S.C. § 103(a) be reversed.

E. 35 U.S.C. § 103(a) Rejections of Claims 2-6

Claims 2-6 depend from and further limit Claim 1. Solely for the purpose of this appeal, Claims 2-6 are not separately argued and will stand or fall with Claim 1.

F. 35 U.S.C. § 103(a) Rejection of Claim 15-20

Claim 15 is similar to Claim 1. Solely for the purpose of this appeal, Claim 15 is not separately argued and will stand or fall with Claim 1.

Claims 16-20 depend from and further limit Claim 15. Solely for the purpose of this appeal, Claims 16-20 are not separately argued and will stand or fall with Claim 1.

G. The Final Rejections of Claims 1-6 and 15-20 Should be Reversed

For the foregoing reasons, it is respectfully submitted that the Final Rejections of Claims 1-6 and 15-20 under 35 U.S.C. § 103(a) are improper. Independent Claims 1 and 15 are not obvious in view of Chu, Kelley, and Barth. Appellant respectfully requests that the rejections of Claims 1-6 and 15-20 be reversed.

Appellant hereby authorizes the Commissioner to charge the required fee for the filing of this Appeal Brief to Deposit Account No. 14-1315 of Nortel Networks Limited. Appellant further requests an extension of time for filing this Appeal Brief, and hereby authorizes the Commissioner to charge the required fee to Deposit Account No. 14-1315 of Nortel Networks Limited. Appellant does not believe that any other fees are due; however, in the event that any other fees are due, the Commissioner is hereby authorized to charge any required fees due (other than issue fees), and to credit any overpayment made, in connection with the filing of this paper to Deposit Account No. 14-1315 of Nortel Networks Limited.

Respectfully submitted,

CARR LLP

Dated: June 15, 2010
CARR LLP
670 Founders Square
900 Jackson Street
Dallas, Texas 75202
Telephone: (214) 760-3030
Fax: (214) 760-3003

/Gregory W. Carr/
Gregory W. Carr
Reg. No. 31,093

VIII. CLAIMS APPENDIX

1. A method of determining an Internet Protocol (IP) address of an application server in a visited serving network, comprising:

receiving an IP address associated with a device on the network by a wireless mobile device;

performing a reverse domain name query by the wireless mobile device using the received IP address;

receiving, by the wireless mobile device, a response to the reverse domain name query comprising the visited serving network domain name, wherein the network is visited by the wireless mobile device and serving the wireless mobile device;

extracting, by the wireless mobile device, the serving network domain name from the received reverse domain name query;

selecting, by the wireless mobile device, an application server name as a function of a service desired by the wireless mobile device;

appending, by the wireless mobile device, the extracted serving network domain name to the application server name, thereby generating a domain-specific application server name;

performing, by the wireless mobile device, a domain name query using the domain-specific application server name; and

receiving, by the wireless mobile device, a response to the domain name query comprising a second IP address, the second IP address identifying an application server in the visited serving network, the application server capable of providing the service desired by the wireless mobile device.

2. The method of Claim 1, wherein receiving an IP address comprises receiving an IP address for the wireless mobile device.

3. The method of Claim 1, wherein receiving an IP address comprises receiving an IP address associated with a device providing an IP address to the serving network.

4. The method of Claim 3, wherein receiving an IP address associated with a device providing an IP address to the serving network comprises receiving an IP address of an access gateway.

5. The method of Claim 1, wherein the step of deriving the serving network domain name information from the reverse domain name query further comprises deriving information from a Uniform Resource Identifier (URI).

6. The method of Claim 1, wherein the application server name comprises a Proxy Call Session Control Function (P-CSCF) server name.

7-14. (Canceled)

15. A system for determining an Internet Protocol (IP) address of an application server in a visited serving network, comprising:

a wireless mobile device in communication with an access gateway of the serving network, wherein the wireless mobile device is configured to:

request an IP address associated with a device on the network from the serving network;

receive the requested IP address;

perform a reverse domain name query using the received IP address;

receive a response to the reverse domain name query comprising the visited serving network domain name, wherein the network is visited by the wireless mobile device and serving the wireless mobile device;

extract the serving network domain name information from the reverse domain name query;

select an application server name as a function of a service desired by the wireless mobile device;

append the extracted serving network domain name information to the application server name, thereby generating a domain-specific application server name;

perform a domain name query using the domain-specific application server name; and

receive a response to the domain name query comprising a second IP address, the second IP address identifying an application server in the visiting serving network, the application server capable of providing the service desired by the wireless mobile device.

16. The system of Claim 15, wherein the serving network has a URI.

17. The system of Claim 15, wherein the IP address is the IP address of the wireless mobile device.

18. The system of Claim 15, wherein the IP address is the IP address of a device providing an IP address to the serving network.

19. The system of Claim 18, wherein the device providing an IP address to the serving network comprises the access gateway.

20. The system of Claim 15, wherein the wireless mobile device is configured to store the second IP address.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.